EXHIBIT 9

How Criminals Recruit Telecom Employees to Help Them Hijack SIM Cards

Sources who work for some of America's major cellphone carriers tell us how criminals are trying to recruit them to help find new targets.

By Lorenzo Franceschi-Bicchierai

August 3, 2018, 11:00am

IMAGE: SHUTTERSTOCK

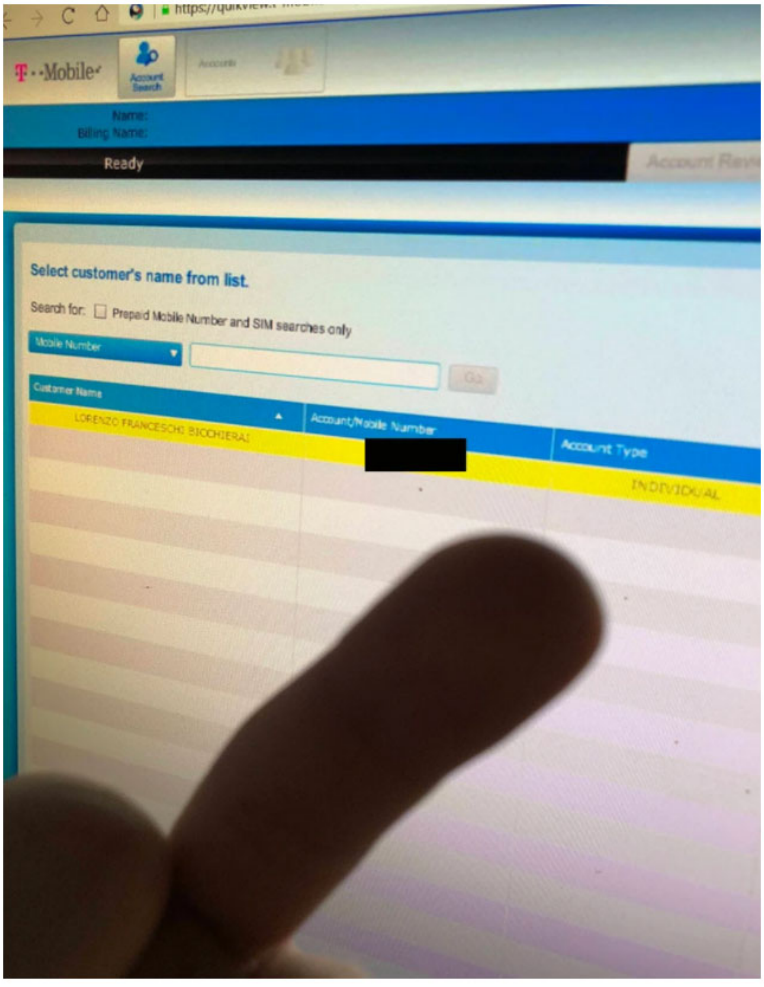
Last year, Joseph Dixon* posted a picture of himself on Instagram, tagging it #T-Mobile, the company he works for as a store manager. The photo gathered a fair amount of likes, and also got the attention of someone who had an unusual business proposal.

"Do you wanna make some money?" the person—a would-be scammer—wrote in an Instagram private message, according to Dixon. (*Dixon's name has been changed because he was not authorized by T-Mobile to speak to the press.)

“Do you wanna make some money?”

The deal was simple: the person would send Dixon the name, phone number, personal details of a T-Mobile customer such as SSN and home address along with the number of a new SIM card. Dixon would then log into T-Mobile’s online employee portal for customer service, called Quickview, transfer that phone number to the new SIM card and collect $100 in Bitcoin.

“I’ll be able to get at least 10 [targets] a week or more,” the would-be scammer wrote Dixon, meaning that Dixon could make up to $1,000 per week.



A SCREENSHOT OF THE AUTHOR'S T-MOBILE ACCOUNT WITHIN QUICKVIEW. THIS SCREENSHOT WAS SHARED BY SOMEONE WHO CLAIMED TO BE A CRIMINAL WITH ACCESS TO THE PORTAL.

In other words, this person was asking Dixon to do SIM swaps for him. A SIM swap is when a cellphone carrier transfers a phone number to a new SIM card. This happens all the time for legitimate reasons when customers change phones or carriers and want to keep their number, or when they lose their phone.

In recent years, however, criminals have used this technique to hijack victims' phone numbers with the goal of stealing their cryptocurrency or unique Instagram handles.

As a recent Motherboard investigation showed, hundreds of people across the US have had their cellphone number hijacked in this so-called "Port Out Scam." Victims have had their emails and social media accounts hacked, and sometimes lost hundreds of thousands of dollars. A 20-year-old college student is accused of being part of a gang that stole more than $5 million by hijacking phone numbers of people involved in the blockchain and cryptocurrency world.

> ***Read more: How To Protect Yourself From SIM Swapping Hacks***

Sometimes, criminals perform these hacks by tricking customer representatives into believing they are the targets. Other times, according to several people involved in the SIM hijacking community, researchers who have investigated it, and one recent reported case, criminals use what they call "plugs": telecom company insiders who get paid to perform illegal swaps.

"Everyone uses them," someone who claimed to be a SIM hijacker told me in a recent chat. "When you tell someone they can make money, they do it."

How criminals find the employees in the first place can vary. Some SIM hijackers I spoke to told me they approach them through shared friends in real life, others told me they just comb LinkedIn, Reddit or social media sites, such as it happened with Dixon.

AT&T and Sprint did not respond to requests for comment about whether or not it had any knowledge of insiders helping criminals. A T-Mobile spokesperson said in a statement that the company is "aware of these ongoing and ever-changing attempts to take advantage of consumers across the wireless industry and we'll keep fighting to ensure our customers' safety." A Verizon spokesperson said the company doesn't share details of internal security processes or investigations, but the company "has systems in place that work to detect employee/vendor misconduct."

> ***Do you work for a cellphone carrier and you have been offered money to help fraudsters? We want to hear your story. No need for names. You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzo@motherboard.tv***

A Verizon employee, who asked to remain anonymous because they were not authorized to speak to the press, told me that a few weeks ago someone approached them via Reddit, offering bribes in exchange for SIM swaps. The employee declined, because they preferred "to stay out of jail," and because the internal system logs every time an employee accesses an account.

"We can literally make $100,000 in a few months," the criminal told another Verizon employee through Reddit. "All I need you to do is either activate the SIM cards for me when you're at work or give me your Employee ID and PIN."

The second employee, who also asked to remain anonymous, brushed him off.

"My employee ID is: Go. And my PIN is: Fuck yourself," they answered, according to a screenshot of the conversation they shared with Motherboard.

> **"T-Mobile has had this issue for years and they seem to not be doing anything about it."**

An employee who works for AT&T told me that if a criminal finds a corrupt insider, "there aren't enough safeguards to stop that employee," in his opinion. The employee himself said he has not been approached, and has no direct experience with SIM swapping fraud, but said the system is designed so that some employees have the ability to override security features such as the phone passcode that AT&T (and other companies) now require when porting numbers.

"From there the passcode can be changed," the employee said in an online chat, referring to a customer information portal that they showed Motherboard. "With a fresh passcode the number can be ported out with no hang ups."

Dixon entertained the criminal's proposal, given that it sounded like an easy job.

"Any T-Mobile rep can go into the account and just change the SIMs. That's part of what T-mobile gives us access to," Dixon told me in a phone call.

In fact, Dixon explained, he could even bypass the regular requirements for porting numbers.

“There’s no passwords needed, there's no ID needed, I can access any account,” he said.

He said he eventually declined the offer because he thought it was unethical, and Dixon himself had seen the damage these scams can do. In the last year, he said he’s had “one or two customers per week saying 'my line is not working' and I look at their account and it says ported. Right away I knew exactly what had happened.”

“This is not new,” Dixon told me, referring to SIM swapping. “T-Mobile has had this issue for years and they seem to not be doing anything about it.”

It’s unclear how long these “plugs” last. In theory, carriers should have systems in place to check which employee was behind an unauthorized port out or SIM swap. Moe The God, a hacker who recently took over the Twitter account of a pro wrestler by hijacking his phone number, told me he has one insider at AT&T and one at Verizon. The first has been working for him since February, the second one since April.

“I just pay them,” the hacker told me in an online chat.

This story has been updated to add quotes from a hacker who goes by Moe The God.